RETAIL EFT (ATM AND POS) CHAPTER 20

(FILE NAME ON DISK # 2 = S2C20.WPD)

Automation has enabled banks to electronically perform many retail banking functions formerly handled manually by tellers, bookkeepers, data entry clerks and other banking personnel. Examples of retail Electronic Funds Transfer (EFT) systems include automated teller machines (ATM), point-of-sale (POS) networks, debit and smart cards, and home banking. Accordingly, the need for physical banking facilities and related staff has been reduced. EFT and related banking services also has brought access to, and control of, accounts closer to the consumer through use of widely distributed unstaffed terminals and merchant facilities. EFT related risk to a financial institution for individual customer transactions is generally low, since the transactions are usually for relatively small amounts. However, weaknesses in controls that could lead to incorrect or improper use of several accounts could lead to significant losses or class action suits to a financial institution. Examinations of retail EFT facilities should focus on the potential large scale risks of a given product.

As with other EFT services, financial institutions have found it beneficial to share their ATM and POS systems' costs and realize economies of scale. This has led some institutions to form alliances that are mutually beneficial. Two examples are:

- Shared systems – A group of financial institutions mutually research, install, market and operate the system.

- Interchange systems – Separate institutions with ATM programs or separate shared systems allow each other's customers use of their machines.

Additionally, there are single institution systems, where only the customers of the bank that developed and installed the ATM system may use the machine.

Fraud, robbery and malfunction are the major risks in an ATM environment. Although the use of plastic cards and PINs act as a deterrent, there is a risk that an unauthorized individual may obtain them. Customers even may be physically accosted while making withdrawals or deposits at ATM locations. Some institutions have decreased this risk by installing surveillance cameras and access/entry control devices.

AUTOMATED TELLER MACHINES (ATM)

An ATM is an EFT terminal that is capable of performing many routine banking services for the customer. ATMs handle deposits, transfers between savings and checking accounts, balance inquiries, withdrawals, small short-term loans and payments to third parties. ATMs usually operate 24 hours a day and are located both on and off bank premises. Daily withdrawals are normally limited to relatively small amounts (usually $500 or less). Deposits are processed in the same manner as if handled by a teller.

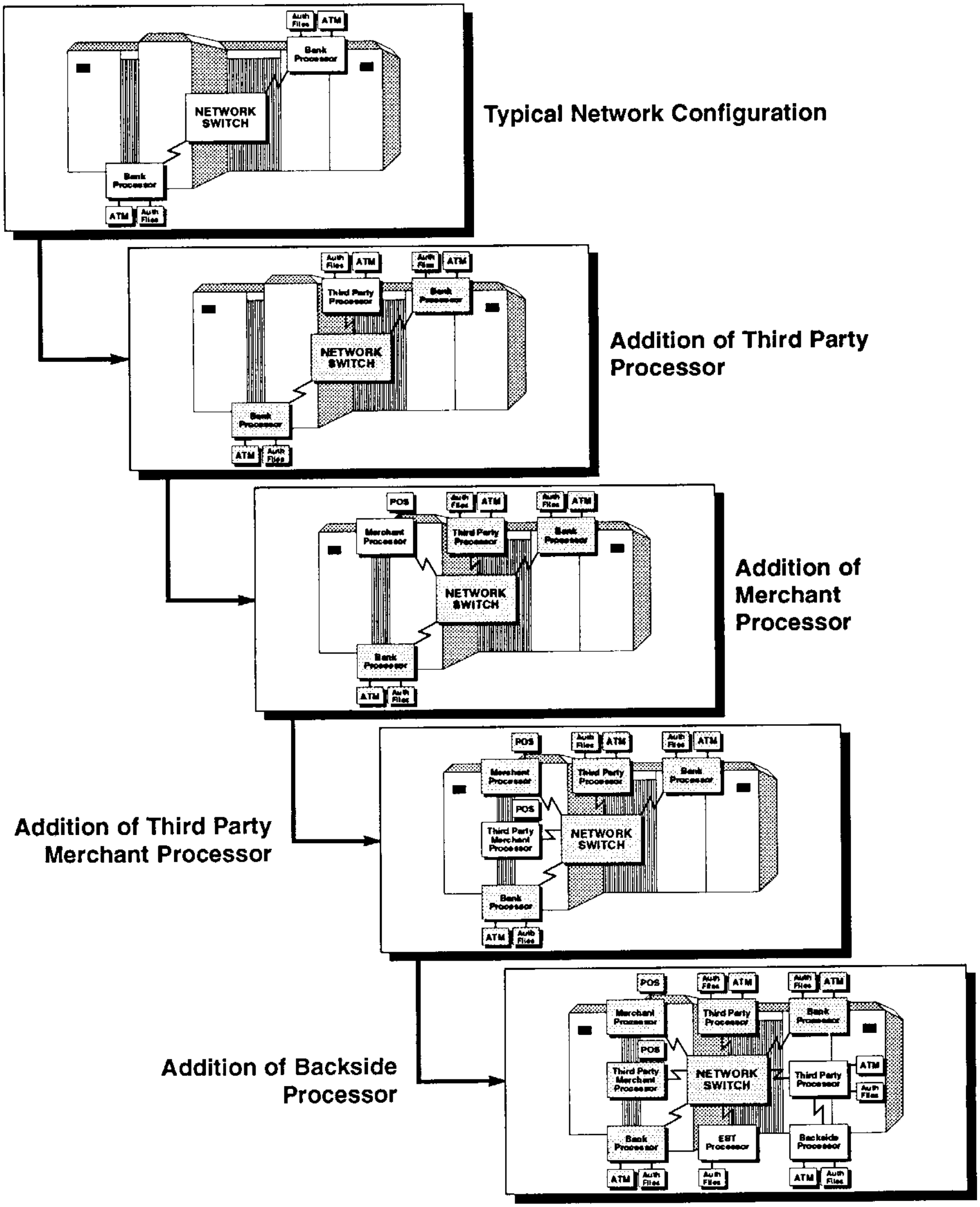
ATMs are generally activated through use of a plastic card encoded with a machine readable customer identification number. In most systems, the customer is required to enter a corresponding personal identification number (PIN).

ATM machines operate in either off-line or on-line mode. Off-line transactions are recorded on tape and physically transported to the financial institution for daily processing. Since off-line systems are not directly connected to the financial institution's computer system, balance verification is normally limited to the customer's opening balance. On-line systems are directly connected to a financial institution's computer system. The computer processes each transaction immediately and provides instant account balance verification. On either system, a card is normally captured if misuse is indicated (e.g., reported stolen or improper PIN number).

POINT-OF-SALE SYSTEMS (POS)

A POS system transaction is defined as an electronic transfer of funds from a customer's checking or savings account to a merchant's account to pay for goods or services. Transactions are initiated from

Figure 20.1
ATM Networks Continue to Increase in Complexity


Typical Network Configuration
Addition of Third Party Processor
Addition of Merchant Processor
Addition of Third Party Merchant Processor
Addition of Backside Processor
NETWORK SWITCH
Bank Processor
Third Party Processor
Merchant Processor
Third Party Merchant Processor
Backside Processor
EFT Processor
ATM
Auth Files
POS

With Permission S. Paur, Pulse EFT Association

POS terminals located in department stores, supermarkets, gasoline stations, and other retail outlets. In an electronic POS system, a customer pays for purchases using a plastic card (e.g., ATM card or debit card). The store clerk enters the payment information into the POS terminal and the customer verifies the transaction by entering a PIN. This results in an automatic debit to the customer's account and credit the merchant.

POS transactions may either be processed through single-institution unshared systems or multi-institution shared networks. Participants in a shared systems settle daily, on a net transaction basis, between each other. In unshared systems, the merchants and customers have accounts with the same financial institution. Thus, the need to settle for transfer of funds between banks is eliminated.

As with other EFT systems, POS transactions are subject to risk of loss due to fraud, mistakes, and system malfunction. POS fraud is caused by stolen cards and PINs, counterfeit cards, and direct computer access. The system also is susceptible to errors such as debiting or crediting an account by too much or too little and entering unauthorized transactions. For the most part, POS systems usually deal with these risks by executing bank-merchant and bank-customer contracts that delineate each party's liabilities and responsibilities. Also, consumers are protected by state and federal statutes limiting their liability if they give notice of a lost, stolen or mutilated card within a specified time period. Another risk inherent in POS systems is that of computer malfunction or downtime. Also, financial institutions offering POS services should provide for adequate records backup.

DEBIT AND SMART CARDS

Other funds transfer related activities that use plastic card and PIN access are debit cards and smart cards. While not EFT systems by themselves, they may be used in conjunction with EFT systems. Debit cards may draw against available balances or lines of credit in related deposit accounts. They can be used for currency withdrawals by ATMs or for the direct purchase of goods or services from retailers using POS or paper-based settlement systems.

Smart cards contain a microchip which can store customer account profiles and credit line balances, as well as a record of transactions. When the card is used to make a purchase, the amount of the purchase is deducted from the balance remaining in the card's memory. Once the credit line in the card is exhausted, it can be replenished. Smart cards do not require on-line terminals.

HOME BANKING

Home banking allows customers to determine their bank account balances, make bill payments, and transfer funds between the customer's own bank accounts via telecommunications lines. These services, which were originally performed solely by telephone, may employ either telephone or personal computers (PCs). To access the account, the customer dials a designated phone number and enters an account number and PIN. If a transfer is to be made, the customer also enters the merchants' identification numbers, customer's account number with each merchant, and the amount and date of payment. If a telephone is used, the data is called back via voice response equipment or, if by computer, the data is transmitted back to the computer terminal screen. The customer then presses a designated key to confirm the transaction. Financial institutions complete the transaction by:

- Transferring funds directly from the customers' account to the merchant accounts, if the accounts are in the same bank.

- Transferring funds into a holding account and sending a check and printout to the merchants.

- Transferring funds to the merchants' bank.

- Transferring funds to a third party who then pays the merchant or utility.

In addition to financial services, some home banking systems include programs that offer such things as:

- Stock brokerage services.

- Home information services that allow electronic access to local and regional newspapers, classified ads, and airline, restaurant, theater and sporting event reservations.

- Income tax preparation service.

INTERNAL CONTROLS FOR RETAIL EFT

Regardless of the system employed, financial institutions should ensure that adequate internal controls are in place to minimize errors, discourage fraud, and provide an adequate audit trail. Recommended internal control guidelines include:

For all systems:

- Measures to establish proper customer identification (PINs) and maintenance of their confidentiality.

- Issuance of a receipt to the customer as required by Regulation E.

- Installing a dependable file maintenance and retention system to trace transactions.

- Producing, reviewing and maintaining exception reports to provide an audit trail.

- Requiring customers of each service to sign agreements that clearly define the responsibilities of the customer and the financial institution.

- Producing and forwarding periodic customers' statements so they can review transactions made during the period and detect unauthorized transfers, as required by Regulation E.

- Confidentiality and security of customer account information including protection of PINs.

- Maintenance of contracts between bank and merchants, customer and banks, and banks and network.

- Daily reconciliation of ATM machine transactions.

- Policies and procedures regarding credit and check authorization, floor limits, override, settlement and balancing.

- Maintenance of transaction journals to provide an adequate audit trail.

- Generation and review of daily exception reports with provisions for follow-up of exception items.

- Provisions for backup and contingency planning.

- Adequate control of captured cards.

- Physical security surrounding ATM terminals.

For transfer and bill paying systems:

- Allow customers to pay bills or transfer funds only from their accounts.

- Require that all transactions be preauthorized for specifically stated customer accounts.

- Discourage payments to third parties without written authorization.

The most critical element of EFT systems is the need for undisputed identification of the customer. Particular attention should be given to the customer identification systems. The most common control is the issuance of a unique PIN that is used with a plastic card or, for non-card systems, an account number. The following guidelines, as recommended by the American Bankers Association, are encouraged.

PIN CONTROL GUIDELINES

Storage

- Unissued PINs should never be stored before issuance They should be calculated when issued and any temporary computer storage areas used in the calculation should be cleared immediately after use.

- PINs should be encrypted on all files and data bases.

- All file maintenance to PINs stored in databases should be restricted. Console logs and/or security reports should be reviewed to determine any attempts to subvert the PIN security system.

Delivery

- PINs should not appear in printed form where they can be associated with customers' account numbers.

- Bank personnel should not be able to retrieve or display customers' PIN numbers via terminals.

- PIN mailers should be processed and delivered with the same security accorded the delivery of bank cards to cardholders. (Note: PINs should never be mailed to a customer together with the card.)

Usage

- The PIN should be entered only by the card-holder and only in an environment that deters casual entry observation.

- The PIN should never be transmitted in unencrypted form.

- PIN systems should record the number of unsuccessful PIN entries and should restrict access to a customer's account after a small number of attempts.

- If a PIN is forgotten, the customer should select a new one rather than having bank personnel retrieve the old one.

Control and security

- Systems should be designed, tested and controlled to preclude retrieval of stored PINs in any non-encrypted form.

- Application programs and other software containing formulas, algorithms, and data used to calculate PINs must be subject to the highest level of access for security purposes.

- Any data recording medium, e.g., magnetic tape and removable disks, used in the process of assigning, distributing, calculating or encrypting PINs must be cleared immediately after use.

- Employees with access to PIN information must be subject to security clearance and must be covered by an adequate surety bond. They should not be involved in card issuance operations in any way.

System design

- To limit fraud, PIN systems should be designed so that PINs can be changed without reissuance of cards.

- PINs used on interchange systems should be designed so that they can be used or changed without any modification to other participants' systems.

- Financial institutions electing to use encryption as a security technique for bank card systems are strongly encouraged to consider the Data Encryption Standards established by the National Bureau of Standards.

PLASTIC CARD CONTROL GUIDELINES

Procurement

- A written agreement between the card manufacturer and the financial institution should detail control procedures and methods of resolution to be followed if problems occur.

- Financial institutions should acquire the card manufacturer's latest third-party audit report.

- An investigation of the security devices used by the manufacturer when encoding and embossing the card should be conducted.

Embossing/Encoding

- If done by a vendor, similar precautions as detailed for card manufacturers should be considered, including written contracts and reviews of control procedures in effect.

- If done on site, the equipment should be maintained in an extremely secure area.

- Proper inventory controls over blank plastic card stock should be in place. There should be proper accounting for the number of cards used, including test cards and spoiled cards.

- Separation and rotation of duties should be practiced to the extent practical and supervisory control reviews should be conducted on a periodic basis.

Storage

- Dual control procedures should be in place. Only a limited working supply of blank cards and cards in the process of being embossed/encoded should be allowed out of the dual custody. Adequate interim storage and accounting must exist for all cards not under dual control.

- Adequate controls should exist for captured cards.

Mailing

- Accountability controls should be created to ensure that all cards initially disbursed from the storage area are delivered to the mail area or are properly destroyed.

- Returned cards should be separately handled by a function independent of the mail department.

- Control cards should be mailed randomly to customers and their delivery validated within a few days to ensure that no theft has taken place.

TERMINAL SHARING/NETWORK SWITCHING

In an attempt to lower costs and provide widespread services, financial institutions share EFT facilities to process retail EFT services, primarily ATM and POS facilities. Some financial institutions are required by state law to share such facilities, while others voluntarily share them. EFT facilities are usually shared regionally; others voluntarily share them on a regional, nationwide and, in some cases, international basis. The most commonly shared EFT systems are:

- An EFT network formed and shared by different financial institutions.

- A multi-bank holding company network servicing affiliated banks.

- A single institution's proprietary EFT network shared with other institutions for a fee.

To facilitate use of the system, a switching network (switch) must be in place to allow shared terminals and computers to communicate with each other. The two types of switching networks used are:

- Line switching – essages are sent directly from one station to another when the central switching site establishes the connection. These systems are commonly used in real-time environments.

- Store and forward – The central switching site stores incoming messages and later retransmits the messages to their destination.

Control Requirements

The primary concerns in shared EFT facilities are security and confidentiality of customer data. These concerns become critical when the network, or any section of it, becomes inoperable or when line problems develop that interrupt the normal transfer of information through the switch. Therefore, adequate audit trails must exist for all transactions, at each switch point, identifying the originating terminal and destination.

Adequate procedures must be in place to control activity if the shared system becomes inoperable to ensure accurate posting and maintain security. Also, procedures for balancing and settling transactions should be well-documented and monitored for adherence. Each participant in the switch should receive adequate transaction journals and exception reports necessary to facilitate final settlement for their institution.

Agreements between switch or network participants must delineate each party's liabilities and responsibilities. Certain basic control items concerning normal and contingency processing must be detailed and responsibility for correction must be stated. Grievance procedures and arbitration policies should be established in order to resolve differences.

Reference is made to the Chapter 18 - Wholesale EFT for consideration of other retail EFT related concerns in the areas of input/output controls, encryption, backup, insurance, disaster recovery, and government regulations. For additional guidance also refer to the Federal Reserve’s *Guide to the Federal Reserve's Payments System Risk Policy*.